

REMARKS

Claims 1-17 are currently active. Claim 17 has been added.

Claims 1 and 2 have been amended. Antecedent support for the amendment is found on page 42, lines 12-44, and device B, device C and device D being 3 computing devices; and for "directly" in Claim 1 from Claim 2. For instance, in the example provided on page 42, line 12 through page 44, line 2, a review of this text shows that device A, device B, device C and device D independently communicate with each other and make their own determination to provide keys without any reference to the host device. Alternatively, see page 38, line 16 through page 40, line 22 where the host computing device is referred to on page 39, line 7 and device A is identified on page 39, line 15 and device B is referred to on page 40, line 6. In all these instances, the device A, device B, device C or device D or any of the devices other than the host computing device independently communicate with each other without the need to receive any type of authorization with the host device.

The Examiner has rejected Claims 1-4 and 9-16 as being unpatentable over Olson in view of Ballardie. Applicants respectfully traverse this rejection.

Olson is a centralized peer-to-peer network, exactly the type of network from which applicants distinguish themselves. Applicants' claimed invention is a decentralized

trusted peer-to-peer network. As stated in the background of the invention, on page 1, lines 24-27, of the above-identified patent application, trusted peer-to-peer networks have relied on a centralized process to establish a trusted peer-to-peer network, in contrast to applicants' decentralized claimed invention.

In a centralized peer-to-peer network, a central host device basically controls the interactions of the other devices in the network. In contrast, in a decentralized peer-to-peer network, each device operates essentially independent of all the other devices. The former, is the structure of Olson, and for that matter Matyas, while the latter is a structure of applicants' claimed invention.

Olson, being a decentralized peer-to-peer network, can be seen from the teachings in Olson that the host client assigns the application session a name and password, and can set settings and operating criteria for the session, such as the maximum number of players permitted. The host client also coordinates and controls the addition of new clients into the application session. It is also the responsibility of the host to allocate unique identifiers to the client admitted into the application session, and to allocate identifiers to any players and/or groups created by other clients. See column 6, lines 50-60. Olson teaches that the host client is the first client in the application session, and is the client that will be responsible for admitting new clients into the session. See column 6, line 67 through column 7, line 3. Olson teaches that the host will typically assign a name for that particular session,

and will then entertain requests from other clients on the network to be admitted into that application session. Other clients on the network 12 who are interested in participating in an application session may utilize available network protocols to seek out an existing host client. The client must request admission of the host for admission to the application session. See column 7, lines 10-16. Olson teaches that the host client will monitor and coordinate the admission of network connected clients seeking to participate in the application session. See column 7, lines 20-23. The host client processor monitors whether any network connected clients are requesting admission into the application session created by the host client. See column 7, lines 25-28. The host will admit the client into the application session depending on certain predefined criteria. See column 7, lines 33-36. If any applicable criteria are not met, the host client processor will deny access to the requesting client and return to the main section of the program code. If the admission criteria are met, the host client will permit the client into the application session by performing a series of functional steps beginning at program step 42 of figure 2b. See column 7, lines 45-50.

Consequently, it is very clear from these teachings that the host client is taught to control who is admitted into a session and who is not, with the client itself totally subject to the control of the host device. Olson is a centralized network.

In contrast, applicants' claimed invention is specifically "a decentralized trusted communications network". The limitation "decentralized" in and of itself distinguishes over

Olson and the applied art of record. However, to further make clear this distinction, Claim 1 has been amended to include the limitation that "a second computer either accepting or denying the public key in regards to joining the decentralized trusted network". This teaching does not exist in Olson. This is because Olson teaches that the client must request admission to the host client. Thus, this is the opposite of applicants' claimed invention. In applicants' claimed invention, it is the second computer that has control over whether it will become part of the network, while in Olson, it is the host client that has control over whether or not the client will be allowed entry into the session. In other words, the client would never request admission into a session and then once given admission, turn it down. Consequently, Olson actually teaches away from applicants' claimed invention because Olson teaches a centralized network and teaches that the client must receive permission from the host client, while in applicants' claimed invention, there is a decentralized trusted network where the second computer has control whether it is going to enter the network or not.

Referring to Ballardie, there is disclosed scalable multicast key distribution. As the title suggests of Ballardie, the teachings are focused on multicast, and how to provide secure multicast in an ever expanding network. In other words, the technique is scalable to a network that has routers that are added to it. Applicants respectfully emphasize the fact that the teachings of Ballardie have to do with multicast. Multicast is a well-known, well-defined technique where a signal from a source node or host is repeated and distributed to many destination nodes throughout a network without necessarily the need for an MCU. Multicast is

a one directional process in terms of the signal that is being multicast. The whole focus of Ballardie is in regard to multicast and how a connection is formed to distribute that signal from the host to the destination nodes securely.

The teachings of Ballardie regarding multicast have nothing at all to do with a decentralized or a centralized network. Ballardie teaches how to distribute a token from a host H to the core router C which, as shown in figure 1, is the key distribution center for the multicast signal to be distributed along the branches of the tree. It is taught on page 7 of Ballardie, the host H first contacts the router A to send a join request to router B, which includes its own unsigned token and the token of H and sends the request to the best next-hop on the path to the core C; the best next hop is router B. B verifies these join requests and then B repeats the aforementioned process except the join is sent from B to C. C authenticates B's join request. Once B and A have been verified, C forms a group access package which includes a token in an encapsulated joined acknowledgment. Two pairs of keys are included in the group access package, one for the originating host, and one for the next hop router to which the join acknowledgment is destined. See page 8 of Ballardie. The group access package is then sent back to B and from B to A. From A the key is set to H thus forming the entire path along which the signal is to be multicast from H is to be sent. If paths and nodes fail, a new route for the core is gleaned as normal from the underlying unicast routing table, and the re-joining process occurs in the same secure fashion. See page 9 of Ballardie.

It is respectfully submitted that is all that Ballardie teaches. Ballardie does teach how to distribute a key to nodes of a path. However, Ballardie does not teach a decentralized network of any type where each computing device can communicate with all the other computing devices on the trusted peer-to-peer network. In a multicast path, the source node can communicate with all the destination nodes, but the destination nodes cannot communicate with all the other destination nodes. The description of how the keys are passed from one node to the other only shows how one node communicates with another node along the path back to the source node. There is no teaching or suggestion of how to communicate from the destination node the key to another destination node. It is not necessary to do so, because in multicast the direction of the signal flows only one way and all that needs to happen regarding the key, is that it is distributed to all the nodes in the path. Accordingly, Ballardie does not add anything at all to the teachings of Olson to arrive at any other claims, as amended, of applicants.

The Examiner has indicated that Claims 5-8 would be allowable if rewritten with the limitations of their base claim on any intervening claims. Newly added Claim 17 is Claim 5 rewritten as such.

Accordingly, the applied art of record fails to teach or suggest a decentralized trusted communications network. Furthermore, the applied art of record does not teach or suggest a second computer either accepting or denying the public key in regards to joining the

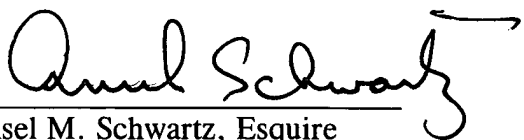
decentralized trusted network. Claim 1 is patentable over the applied art of record. Claim 2 is patentable for the reasons Claim 1 is patentable.

Claims 3-8 are dependent to parent Claim 2 and are patentable for the reasons Claim 2 is patentable. Claims 9 to 12 are dependent to parent Claim 1 and are patentable for the reasons Claim 1 is patentable.

Claims 13-16 have the limitation of a "decentralized peer-to-peer network" and are patentable over the applied art of record.

In view of the foregoing amendments and remarks, it is respectfully requested that the outstanding rejections and objections to this application be reconsidered and withdrawn, and Claims 1-17, now in this application be allowed.

Respectfully submitted,

By 

Ansel M. Schwartz, Esquire
Reg. No. 30,587
One Sterling Plaza
201 N. Craig Street, Suite 304
Pittsburgh, PA 15213
(412) 621-9222

Attorney for Applicants